ON THE SIMPLE GROUP OF D. G. HIGMAN AND C. C. SIMS

BY

GRAHAM HIGMAN

1. Introduction

Higman and Sims [3] describe their group as a permutation group of rank 3 and degree 100, in which the stabiliser of a point is a Mathieu group M_{22}, and has orbits of lengths 1, 22 and 77. Here we shall exhibit what is presumably the same group as a doubly transitive permutation group of degree 176, in which the stabiliser of a point is an extension by a field automorphism of the projective unitary group $PSU(3, 5^2)$. (We shall denote this extension by $P\Sigma U(3, 5^2)$.)

We shall construct a "geometry" of which the group is the automorphism group. We shall call the objects of the geometry points, conics and quadrics, since these seem to be the simplest objects of ordinary geometry which could possibly realize the required configuration; though I do not know that it can be realized in any projective space. The geometry has the following properties.

   (i)   There are 176 points, 1100 conics and 176 quadrics.

   (ii)   Each quadric contains 50 points, and each point is on 50 quadrics.

   (iii)   Each conic contains 8 points and lies on 8 quadrics.

   (iv)   Through any two points there pass just two conics; any quadric through both points contains at least one of the conics; and just two quadrics contain both conics.

   (v)   On any two quadrics there lie just two conics; any point on both quadrics lies on at least one of the conics; and there are just two points lying on both conics.

   (vi)   A conic S determines a one to one correspondence between the points q on it and the quadrics Q through it, such that, if q corresponds to Q,

         (α)   The conics S' meeting S in two points, one of which is q, lie on Q;

         (β)   The conics S' lying on two quadrics through S, one of which is Q, contain q.

The automorphism group of the geometry is transitive on conics, on incident point-quadric pairs, and on non-incident point-quadric pairs, and doubly transitive on points and on quadrics. Thus the stabiliser of a point permutes the quadrics in orbits of lengths 50 and 126. On the orbit of length 50, it is a rank 3 group with suborbits of lengths 1, 7 and 42, and so by a result of D. G. Higman [2] is either $PSU(3, 5^2)$, of order 126,000, or $P\Sigma U(3, 5^2)$ of order 252,000. However, the stabiliser of a point-pair is fairly easily seen to have order 2,880, being isomorphic to $Z_2 \times$ Aut (A_6), which implies that the stabiliser of a point has order 252,000, and that the whole group has order

44,352,000. It is almost trivial that the group either is simple or has a simple subgroup of index two, and the second possibility is not hard to rule out. That the group is isomorphic to the Higman-Sims group I have not actually proved, but it seems very likely. Not only are the orders of the groups the same, but there is a one to one correspondence between their conjugacy classes preserving the orders of centralisers, and the groups have the same character table. Moreover the outer automorphism, which in the Higman-Sims representation extends the outer automorphism of M_{22}, is in this representation realized by a polarity of the geometry.

Evidently either the conics or the quadrics of the geometry may be taken as the blocks of a design (in the sense of Hall [1]). Either design determines the geometry, so that the automorphism group of the design is the automorphism group of the geometry. My first proof of the existence of this doubly transitive group used only the unsymmetric design formed by the conics: I owe to D. R. Hughes the suggestion that there ought also to be a symmetric design with 50 points to a block; and the discovery of this design has eliminated much tedious calculation from the proof. An obvious remaining question is whether there exist other similar geometries, say satisfying (iv), (v) and (vi), but with other numbers in (i), (ii) and (iii), and, if so, what their automorphism groups are. Also, it is clear from conditions (iv) and (v) that if P and Q are sets with 176 elements there is a one to one map θ of the set $P^{(2)}$ of unordered pairs of elements of P onto $Q^{(2)}$, which is not induced by a one to one map of P onto Q, but is nevertheless highly symmetrical, in that the group of pairs (α, β) of permutations of P and Q such that $\alpha^{(2)}\theta = \theta\beta^{(2)}$ is transitive. This situation, too, might be worth trying to generalise.

2. Description of the geometry

We recall first that the symmetric group S_6 has an outer automorphism, which interchanges the classes $(1^4 2)$ and (2^3), $(1^3 3)$ and (3^2), and $(1\ 2\ 3)$ and (6), and leaves the other classes unchanged. If A is a set with 6 elements, we denote by A^* a set also with 6 elements, such that the symmetric group on A acts on A^* also, but in the fashion suggested by the outer automorphism. More precisely, and furthermore, if C is the category whose objects are sets with 6 elements and whose morphisms are one to one mappings, $*$ is to be a functor from C to C. Then, in particular, if α is a permutation of A, α^* is a permutation of A^*, and if ρ is a one to one map from A to A^*, the map carrying α to $\rho\alpha^*\rho^{-1}$ is an endomorphism of the symmetric group on A: we require this endomorphism to be an outer automorphism. Of course, A^* can be thought of more concretely as the set of distinct ways in which A can be given the structure of a projective line over $GF(5)$, but we shall make no use of this.

Now let B be a set with 8 elements, and for $a \neq b$ in B, write $[ab]$ for $B \backslash \{a, b\}$. If we assume, as we may, that the 28 sets $[ab]^*$ are dis-

joint from one another and from B, then

$$P = B \cup \bigcup [ab]^*$$

is a set with 176 elements, which will be the points of the geometry. The symmetric group S_8 on B acts as a permutation group on P; if σ belongs to S_8, σ restricted to $[ab]$ is a one to one map σ_{ab} of $[ab]$ onto $[a\sigma, b\sigma]$, and so σ_{ab}^* is a one to one map of $[ab]^*$ onto $[a\sigma, b\sigma]^*$; putting these maps together for different a, b, with the natural action of σ on B, gives a permutation of P which we also denote by σ. We shall define the set Q of quadrics as

$$Q = \{L_u \; ; \quad u \in P\}$$

where, for $a \in B$,

$$L_a = B \cup \bigcup_{b \neq a} [ab]^*$$

and, for $x \in [ab]^*$,

$$L_x = \{a, b\} \cup [ab]^* \cup \{x(ac); c \in [ab]\} \cup \{x(bc); c \in [ab]\}$$

$$\cup \{x(ac)(bd); c \neq d, c, d \in [ab]\}.$$

(Here (ac) is the transposition interchanging a and c, etc.) We shall not describe the conics explicitly; they are the images of B under the automorphism group of the design (P, Q).

It is clear that this automorphism group contains S_8, and the notation has been chosen precisely to make it clear. To exhibit other automorphisms, we translate the description of the geometry into another notation. We choose two elements of B and call them ∞ and 0. We write D for $[\infty 0]$ and so D^* for $[\infty 0]^*$. If $z \in [0a]^*$, for $a \in D$, we write $z = (a, z(\infty a))_1$, thus identifying $\bigcup_a [0a]^*$ with a copy $(D \times D^*)_1$ of the cartesian product of D and D^*. Similarly we identify $\bigcup_a [\infty a]^*$ with a second copy $(D \times D^*)_2$ of the cartesian product, by writing $z = (a, z(0a))_2$, for $z \in [\infty a]^*$. Finally, for $z \in [ab]^*$, a, $b \in D$, we want to identify z with (a, b, x, y), where $x = z(\infty a)(0b)$, $y = z(\infty b)(0a)$. However, since a, b are unordered, this requires us at the same time to identify also (a, b, x, y) with (b, a, y, x). We notice also that x, y are elements of D^* such that $y = x(ab)^*$. So we define E_0 to be the subset of $D \times D \times D^* \times D^*$ consisting of elements (a, b, x, y) such that $a \neq b$ and x, y are interchanged in $(ab)^*$, and E to be the set obtained from E_0 by identifying (a, b, x, y) with (b, a, y, x). Then the set of points, in our new notation, is

$$P = \{0, \infty\} \cup D \cup D^* \cup (D \times D^*)_1 \cup (D \times D^*)_2 \cup E.$$

The notation is designed to bring out the symmetry between D and D^*. It is for this reason that we retain the redundant notation (a, b, x, y) for elements of E_0, though any three of a, b, x, y determine the fourth. For the same reason we shall identify D^{**} with D, as is certainly possible, in such a way that for any permutation α of D, $\alpha^{**} = \alpha$. The defining condition for E_0 is then symmetric: if x, y are interchanged in $(ab)^*$ then a, b are interchanged in $(xy)^*$.

It remains to translate into the new notation the definitions of the quadrics L_u. We find:

(i)
$$L_0 = \{0, \infty\} \cup D \cup D^* \cup (D \times D^*)_1 ,$$
$$L_\infty = \{0, \infty\} \cup D \cup D^* \cup (D \times D^*)_2 .$$

(ii) For $a \in D$,
$$L_\alpha = \{0, \infty\} \cup D \cup (a \times D^*)_1 \cup (a \times D^*)_2 \cup ((a \times D \times D^* \times D^*) \cap E_0);$$

for $x \in D^*$,
$$L_x = \{0, \infty\} \cup D^* \cup (D \times x)_1 \cup (D \times x)_2 \cup ((D \times D \times x \times D^*) \cap E_0).$$

(iii)
$$\begin{aligned}
L_{(a,x)_1} = \{0, a, x\} &\cup (a \times D^*)_1 \cup (D \times x)_2 \\
&\cup \{(b, y)_i ; (a, b, x, y) \in E_0 , i = 1, 2\} \\
&\cup \{(b, c, y, z); (a, b, x, y) \in E_0 \text{ and } (b, c, y, z) \in E_0\}
\end{aligned}$$

$$\begin{aligned}
L_{(a,x)_2} = \{\infty, a, x\} &\cup (D \times x)_1 \cup (a \times D^*)_2 \\
&\cup \{(b, y)_i ; (a, b, x, y) \in E_0 , i = 1, 2\} \\
&\cup \{(b, c, z, y); (a, b, x, y) \in E_0 \text{ and } (b, c, y, z) \in E_0\}.
\end{aligned}$$

(iv)
$$\begin{aligned}
L_{(a,b,x,y)} = \{a, b, x, y\} &\cup \{(c, z)_1 ; (a, c, x, z) \in E_0 \text{ or } (c, b, z, y) \in E_0\} \\
&\cup \{(c, z)_2 ; (a, c, z, y) \in E_0 \text{ or } (c, b, x, z) \in E_0\} \\
&\cup ((a \times b \times D^* \times D^*) \cap E_0) \\
&\cup ((D \times D \times x \times y) \cap E_0) \\
&\cup \{(a, c, u, v); (c, b, x, u) \in E_0 \text{ and } (a, c, u, v) \in E_0\} \\
&\cup \{(c, b, u, v); (a, c, v, y) \in E_0 \text{ and } (c, b, u, v) \in E_0\} \\
&\cup \{(d, e, x, z); (a, e, z, y) \in E_0 \text{ and } (d, e, x, z) \in E_0\} \\
&\cup \{(d, e, z, y); (d, b, x, z) \in E_0 \text{ and } (d, e, z, y) \in E_0\}.
\end{aligned}$$

For the most part these come by straightforward and reasonably short calculation, but in one or two places some manhandling is necessary to get the results into the symmetric form we require. Suppose, for instance, that $w = (a, b, x, y)$, and consider the elements $w(ad)(be)$ of L_w, where $d, e \in D$. A direct calculation gives $w(ad)(be) = (d, e, u, v)$ where

$$u = x(ad)(be)^* = y(aebd)^*,$$
$$v = x(aebd)^* = y(ad)(be)^*.$$

Now choose notation for the complement of $\{a, b\}$ in D so that $(ab)(ij)(kl)^*$ is the transposition (xy). If $d = i, e = j$ then $(ad)(be)^*$ belongs to the class $(1^2 2^2)$ and commutes with (xy). Thus it either fixes x and y or interchanges them. So $w(ad)(be) = (d, e, u, v)$ belongs to $(D \times D \times x \times y) \cap E_0$. But if $d = i, e = k$, then $(ad)(be)^*$ belongs to the class $(1^2 2^2)$ and $(xy) \cdot (ad)(be)^* = (aejbde)^*$ belongs to the class (123). Thus $(ad)(be)^*$ fixes one of x, y, say x. Then $u = x$, and

$$v = u(de)^* = x(de)^* = y(ab)(de)^* = y(abed)(ae)^*.$$

But since $(ad)(be)^*$ fixes x, $(ae)(bd)^*$ fixes $y = x(ab)^*$, and so $(abed)^*$ also

fixes y. Thus $v = y(ae)^*$. Thus $w(ad)(be) = (d, e, u, v)$ belongs to

$$\{(d, e, x, z); (a, e, z, y) \in E_0 \quad \text{and} \quad (d, e, x, z) \in E_0\}.$$

Similarly, one verifies that all elements of L_w belong to the set written down, and, by counting, nothing else does.

3. The automorphism group

We begin our consideration of the automorphism group G of the geometry by showing that the symmetric group S_8 on B is the stabiliser of B in G; that is, that if θ in G stabilises B pointwise then $\theta = 1$.

First the elements of $[ab]^*$ can be characterised among the elements of $P \backslash B$ by the fact that through them there pass more than 4 quadrics (in fact, 8 quadrics) through a and b. This is unaltered by application of θ, so θ stabilises each $[ab]^*$. Let θ_{ab} be the restriction of θ to $[ab]^*$. Again, if $x \in [ab]^*$ and $y \in [bc]^*$, there are more than 3 quadrics through a, x, and y only if $y = x(ac)$, which it is more convenient now to write $y = x\delta^*(ab, bc)$, where $\delta(ab, bc)$ is the unique one to one map of $[ab]$ onto $[bc]$ which is the identity on their intersection. If there are more than 3 quadrics through a, x, y there are more than 3 through a, $x\theta$, $y\theta$, so that

$$\theta_{ab} \, \delta^*(ab, bc) = \delta^*(ab, bc)\theta_{bc}.$$

It is easy to see that any permutation σ of $[ab]$ can be written as the composition of a sequence of maps $\delta(de, ef)$; and repeated application of the last equation then shows that θ_{ab} commutes with σ^* for all σ. Thus $\theta_{ab} = 1$, and $\theta = 1$ as required.

Next, consider the stabiliser in G of the point pair $\{0, \infty\}$, in the notation of the second description of the geometry. Obviously the stabiliser contains S_6, the symmetric group on D (or on D^*). It also contains an involution τ which interchanges 0 and ∞, stabilises D and D^* pointwise, interchanges $(a, x)_1$ and $(a, x)_2$, and interchanges (a, b, x, y) and (a, b, y, x). τ centralises S_6, and $\langle \tau \rangle \times S_6$ is the intersection of the stabiliser of $\{0, \infty\}$ with the stabiliser S_8 of $B = \{0, \infty\} \cup D$. Now let φ be a one to one map from D to D^*, so that φ^* maps D^* to D. If x, y are interchanged in $(ab)^*$ then $x\varphi^*$, $y\varphi^*$ are interchanged in $(a\varphi b\varphi)^*$. That is, if (a, b, x, y) belongs to E_0, so does $(x\varphi^*, y\varphi^*, a\varphi, b\varphi)$. From this it follows immediately that there is an automorphism of the geometry, which we shall also call φ, which fixes 0 and ∞, maps a on $a\varphi$ and x on $x\varphi^*$, for $a \in D$, and $x \in D^*$, $(a, x)_1$ on $(x\varphi^*, a\varphi)_2$, $(a, x)_2$ on $(x\varphi^*, a\varphi)_1$, and (a, b, x, y) on $(x\varphi^*, y\varphi^*, a\varphi, b\varphi)$. It is clear that φ centralises τ, and normalises S_6, inducing an outer automorphism in it, so that $\langle \varphi, \tau, S_6 \rangle$ is isomorphic to $Z_2 \times \mathrm{Aut}(S_6)$, and so is of order 2880.

This is the whole stabiliser of $\{0, \infty\}$. For the points in $D \cup D^*$ are the only points u such that there are more than 4 quadrics through 0, ∞ and u; and if a, $b \in D$ the quadrics through 0, ∞ and a and through 0, ∞ and b are the same, whereas different ones go through 0, ∞ and x for $x \in D^*$. Thus an

element of the stabiliser of $\{0, \infty\}$ either stabilises D and D^* or interchanges them. Thus if there is an element of the stabiliser not in $\langle \varphi, \tau, S_6 \rangle$ there is an element not 1 stabilising $\{0, \infty\} \cup D = B$ pointwise, which we have seen is not so.

Notice next that for all u, v in P, $u \in L_v$ is equivalent to $v \in L_u$. That is, the map interchanging u and L_u is a polarity, and so induces an automorphism of G, which interchanges the stabiliser of a point with the stabiliser of a quadric. Since the stabiliser of a point fixes no quadric, this is an outer automorphism. Evidently it centralises S_8, but it is easy to see that it transforms φ into $\varphi\tau$.

The double transitivity of G, on points or on quadrics, is now easy to check. The orbits of S_8 on P are B and $P\backslash B$, and φ interchanges the subsets D of B and D^* of $P\backslash B$, so the group is certainly transitive on points. The stabiliser S_7 of ∞ in S_8 has orbits $\{\infty\}$, $B\backslash\{\infty\}$, $\bigcup_{a\neq\infty}[\infty a]^*$, and $\bigcup_{a,b\neq\infty}[ab]^*$ on P, and φ, which also stabilises ∞, interchanges D in $B\backslash\{\infty\}$ with D^* in $\bigcup_{a\neq\infty}[\infty a]^*$, and $[\infty a]^*$, where $a \neq 0$, in $\bigcup_{a\neq 0}[\infty a]^*$ with $[0a]^*$ in $\bigcup_{a,b\neq\infty}[ab]^*$. This proves the double transitivity.

It now follows, of course, that the order of G is 44,352,000, and the order of a stabiliser of a point 252,000. The properties (i) to (vi) of the geometry, mentioned in the introduction, can also now be checked simply; and since we make no use of them, we leave this to the reader.

Since S_8 acts on quadrics in the same way that it does on points, the orbits on Q of the stabiliser S_7 of ∞ in S_8 are

$$\{L_\infty\}, \quad \{L_a, \ a \in B\backslash\{\infty\}\}, \quad \{L_x ; \ x \in [\infty a]^*, \ a \in B\backslash\{\infty\}\}$$

and

$$\{L_x ; \ x \in [ab]^*, \ a, \ b \in B\backslash\{\infty\}\}.$$

But φ acts differently on the quadrics; in particular, it interchanges L_0 and L_∞, and maps L_a, $a \neq 0$, ∞, on $L_{a\varphi}$. Thus the stabiliser of ∞ permutes transitively the elements of the first three orbits, that is, permutes transitively the 50 quadrics containing ∞. The remaining orbit under S_7 consists of the 126 quadrics not containing ∞. Thus G is transitive on incident point-quadric pairs and on non-incident point-quadric pairs.

The stabiliser of the pair $\{\infty, L_\infty\}$ contains S_7, and by calculating its order we see that it is S_7. Its orbits on the set of quadrics through ∞, as described in the previous paragraph, have lengths 1, 7, 42. That is, the stabiliser of ∞ acts on this set as a rank 3 group with these suborbit lengths. By a result of D. G. Higman [2] and our knowledge of its order, it is $P\Sigma U(3, 5^2)$.

Finally, to prove simplicity, assume that N is a minimal normal subgroup of G. Then N is transitive. Being characteristically simple, it cannot have order 176, so it has non-trivial intersection with the stabiliser $P\Sigma U(3, 5^2)$ of a point. This intersection, being normal, must be either $P\Sigma U(3, 5^2)$ itself or $\mathrm{PSU}(3, 5^2)$. In the first case $N = G$ and G is simple, so we assume that the second holds, so that N is of index 2 in G. Then N is unique and so characteristic, and is doubly transitive. The intersection of N with the stabiliser

of the point pair $\{0, \infty\}$ is of index 2 in the stabiliser, which, we recall, is $\langle \tau \rangle \times \mathrm{Aut}\,(A_6)$. As before we denote by φ an element of $\mathrm{Aut}\,(A_6)$ not in S_6, and we now denote by ψ an element of S_6 not in A_6. Then $\tau\psi$ is an even element of S_8 and so belongs to N. We recall that the polarity of the geometry induces an outer automorphism of G which centralises $\langle \tau \rangle \times S_6$ and maps φ on $\varphi\tau$. This automorphism normalises N, so that if N contains an element $\varphi\alpha$ where $\alpha \,\epsilon\, \langle \tau \rangle \times S_6$ it contains also $\varphi\tau\alpha$, and therefore contains τ, whence the intersection of N with the stabiliser of $\{0, \infty\}$ cannot be of index 2 in the stabiliser. Thus the stabiliser of $\{0, \infty\}$ in N is $\langle \tau \rangle \times S_6$, which stabilises each of the conics $\{0, \infty\} \cup D$ and $\{0, \infty\} \cup D^*$ through $\{0, \infty\}$. Now the double transitivity of N on either conic ensures that if any element of N transforms one conic into the other, an element of the stabiliser does. Thus N permutes the 1100 conics in two orbits of length 550 each, the two conics through any point-pair being in different orbits. It follows that if $S_1, S_2, \cdots, S_n, S_1$ is a closed chain of conics, in which any two consecutive conics have a point pair in common, then n is even. But it is easy to verify that not only B but also $B_{ab} = \{a, b\} \cup [ab]^*$, for $a, b \,\epsilon\, B$, and

$$B_{ax} = \{a, x\} \cup \{x(ac); c \,\epsilon\, [ab]\},$$

for $a \,\epsilon\, B$ and $x \,\epsilon\, [ab]^*$ are conics, and, if $x \,\epsilon\, [ab]^*$ and $y = x(ac)$, then B, B_{ab}, $B_{ax}, B_{cy}, B_{cb}, B$ is such a chain with $n = 5$. Hence G has no normal subgroup of index 2, and hence G is simple.

REFERENCES

1. MARSHALL HALL JR., *Combinatorial theory*, Blaisdell, Waltham, Mass., 1967.
2. D. G. HIGMAN, *Finite permutation group of rank 3*, Math. Zeitschrift, vol. 86 (1964), pp. 146–156.
3. D. G. HIGMAN AND C. C. SIMS, *A simple group of order* 44,352,000, Math. Zeitschrift, vol. 105 (1968), pp. 110–113.

THE MATHEMATICAL INSTITUTE
    OXFORD, ENGLAND